The Dynamics of Terrorist Networks: Understanding the Survival Mechanisms of Global Salafi Jihad

Xu, Jie ; Hu, Daning ; Chen, Hsinchun

Abstract: Today terrorists usually work in network forms to conduct attacks. Terrorist networks remain active and can still function even after being severely damaged by authorities. Analyzing terrorist networks from a dynamic point of view can provide insights about the mechanisms responsible for the survival of terrorist organizations. This paper studies the dynamics of a major international terrorist organization over a 14-year period – the Global Salafi Jihad (GSJ) terrorist network. We found that a scale-free topology gradually emerged as new members joined the GSJ network based on operational needs. In addition, since the network has been experiencing member losses while it grows, we also studied the robustness of the GSJ network. We used a simulation approach to examine its vulnerability to random failures, targeted attacks, and real world authorities' counterattacks. We found that authorities' counterattacks have been rather ineffective in disrupting the terrorist network.

DOI: https://doi.org/10.2202/1547-7355.1477

Journal of Homeland Security and Emergency Management

Volume 6, *Issue* 1 2009 *Article* 27

The Dynamics of Terrorist Networks: Understanding the Survival Mechanisms of Global Salafi Jihad

Jie Xu, *Bentley College*
Daning Hu, *University of Arizona*
Hsinchun Chen, *University of Arizona*

Recommended Citation:
Xu, Jie; Hu, Daning; and Chen, Hsinchun (2009) "The Dynamics of Terrorist Networks: Understanding the Survival Mechanisms of Global Salafi Jihad," *Journal of Homeland Security and Emergency Management*: Vol. 6: Iss. 1, Article 27.
DOI: 10.2202/1547-7355.1477

The Dynamics of Terrorist Networks: Understanding the Survival Mechanisms of Global Salafi Jihad

Jie Xu, Daning Hu, and Hsinchun Chen

Abstract

Today terrorists usually work in network forms to conduct attacks. Terrorist networks remain active and can still function even after being severely damaged by authorities. Analyzing terrorist networks from a dynamic point of view can provide insights about the mechanisms responsible for the survival of terrorist organizations. This paper studies the dynamics of a major international terrorist organization over a 14-year period – the Global Salafi Jihad (GSJ) terrorist network. We found that a scale-free topology gradually emerged as new members joined the GSJ network based on operational needs. In addition, since the network has been experiencing member losses while it grows, we also studied the robustness of the GSJ network. We used a simulation approach to examine its vulnerability to random failures, targeted attacks, and real world authorities' counterattacks. We found that authorities' counterattacks have been rather ineffective in disrupting the terrorist network.

KEYWORDS: social network analysis, network dynamics, network robustness, simulation, terrorist network

Introduction

Terrorism and terrorist attacks seriously threaten national security and public safety in countries around the world. Authorities have been fighting terrorism for a long time, and numerous arrests have damaged major terrorist organizations such as Al Qaeda. However, the tragic events of September 11 in the U.S., the Madrid train bombing in Spain, and the London subway/bus bombings in the United Kingdom indicate that terrorist organizations remain active and can still function even after severe damage. How these terrorist organizations have survived disruption and attacks is a question that has long puzzled authorities and terrorism researchers.

It is conjectured that the structure of terrorist organizations greatly enhances their resistibility and robustness to attacks and damage (Klerks 2001; Krebs 2001). Traditionally, terrorist organizations were believed to have a centralized, hierarchical structure in which the leaders at the top of the hierarchy control the operation of the entire organization. Such a hierarchical structure is more vulnerable to attacks targeting the leaders. Contemporary terrorist organizations have adopted a network structure which is decentralized and more flattened (Klerks 2001; Milward and Raab 2002). In these networks social ties between terrorists hold the organization together and the control of operations is dispersed all over the network. As a result, the network can still function even if some parts of it are destroyed.

Although the conjecture is interesting, there have been few empirical studies that systematically verify it. The structural mechanisms responsible for the survival of terrorist networks remain unknown for two major reasons. First, nearly all theoretical and practical studies on terrorist networks suffer from the lack of empirical data. As terrorist networks are clandestine organizations that operate covertly, data about the individual members and their social ties are extremely difficult to gather. Anecdotal evidence from news stories and media sources is highly unreliable. Second, the dynamic nature of terrorist networks is largely ignored. Terrorist organizations are dynamic systems and undergo constant changes over time (Carley et al. 2003; Dombroski and Carley 2002). On one hand, a network can grow by recruiting new members. New members may join the network through all sorts of social ties such as friendship, kinship, and religion. On the other hand, it may lose its members due to arrests and suicide bombings.

The purpose of this article is to analyze terrorist networks from a dynamic point of view in order to uncover the mechanisms responsible for their survival. Based on a relatively reliable dataset about a major international terrorist organization, Global Salafi Jihad, we aim to answer a series of questions: What is the topology of these networks? How have these networks evolved? How robust

are these networks? How have these networks managed to survive? Have authorities' counterattacks been effective?

The remainder of this article is organized as follows. In the next section we review related literature about network structure and dynamics. The second section introduces the dataset and research methods for this study. We then present and discuss the results. We summarize our findings and conclude the paper in the last section.

Literature Review

Recent development in the topological analysis of large networks (Albert and Barabási 2002) has provided a great opportunity for studying the dynamics of terrorist networks. Examples of networks are the World Wide Web (Broder et al. 2000; Huberman and Adamic 1999; Kumar et al. 1999), the Internet (Faloutsos et al. 1999), movie actor networks in which nodes are actors and links are their collaboration relationships in movies (Watts and Strogatz 1998), coauthorship networks of academic authors who wrote papers together (Newman 2001; Newman 2004), and metabolic pathways that consist of biochemical reactions occurring in a cell (Jeong et al. 2000). One important contribution of such development is its focus on the dynamics of scale-free networks (Barabási and Albert 1999). In a scale-free network, a large percentage of the nodes have only a few links (low degree) while a small percentage of nodes have a very large number of links (high degree), where degree is defined as the number of links a node has.

A scale-free network's structure is significantly different from a random graph network, in which every node has roughly the same number of links. That is, nodes are randomly connected and the network is rather homogeneous in terms of node degree. However, in a scale-free network, there are some "hubs" that connect to a large number of other nodes and hold the network together. The degree distribution, $p(k)$, which plots the probability that an arbitrary node in a network has exactly k links, can clearly show the difference between the two types of network. The degree distribution of a random graph network is a bell-shaped Poison distribution peaking at the average degree, while that of a scale-free network is a highly skewed one that has no peak but a very long, flat tail, which is often called power-law distribution (Albert and Barabási 2002).

It is interesting to study what causes the emergence of the scale-free structure, which is common in many real networks. Various models (Faloutsos et al. 1999; Garlaschelli et al. 2003; Jeong et al. 2000; Newman 2004) have been proposed to uncover the mechanisms responsible for such a highly skewed power-law degree distribution. Among these mechanisms, growth and preferential attachment have been believed to be the two fundamental mechanisms in the evolution of scale-

free networks (Barabási and Albert 1999). Growth means that the size of a network is not fixed. Instead, a network can grow by including new nodes. Preferential attachment means that when a new node is added to the network the probability that an old node receives a link from the new node depends on the number of existing links of the old node, a phenomenon known as "the rich get richer." With both mechanisms the scale-free structure thus is the product of evolution, a dynamic process in nature.

Moreover, some research has studied the robustness of different topologies (random and scale-free) against failures and attacks (Albert et al. 2000; Cohen et al. 2000; Crucitti et al. 2003; Solé and Montoya 2001). Scale-free networks have been found to be very robust against random errors but highly vulnerable to attacks targeting the hubs. Because random errors remove nodes randomly from a network, the majority of the network can remain connected even if it loses a number of low-degree nodes. However, the removal of just a small number of hubs will easily break down the entire network, because the attacks remove not only the hubs but also their links to a large number of low-degree nodes, causing those nodes to be disconnected (Albert et al. 2000).

Although these findings about scale-free networks in general are illuminating, they cannot be applied to terrorist networks in a straightforward manner. Most of these studies assume that a network is either in a growing mode, where the network adds new nodes without losing existing nodes, or in a decaying mode, where some nodes are removed due to failure or attack. However, in reality terrorist networks are seldom in merely one mode. The survival of a terrorist network is actually the product of the mixture of both growing and decaying modes. Some studies have considered aging as a decaying factor during the growth of a network, when nodes naturally drop out of the network after a certain period of time (Amaral et al. 2000). However, for a terrorist network, attack from authorities rather than aging may be the most important decaying factor. No existing findings thus far can be applied to directly account for the survival of terrorist organizations. In addition, because of the lack of large reliable datasets, statistical analysis of the topology of terrorist networks is almost impossible, let alone dynamic analysis which requires information about the time when changes occur to a network.

In this research we focus on the survival process of terrorist networks by studying their evolution and robustness, realizing that they can both grow and be under attack at the same time. We use the Global Salafi Jihad data to study the process and demonstrate our findings. Through this study we hope to contribute to the research on terrorism and counterterrorism policies and to provide insights into the survival mechanisms of large networks in hostile environments.

Data and Methods

We study the Global Salafi Jihad (GSJ) terrorist network (Sageman 2004) which consists of 366 members, including those from Osama Bin Laden's Al Qaeda. These terrorists were connected by kinship, friendship, religious ties, and relations formed after they joined the GSJ network.

The Global Salafi Jihad is part of a violent worldwide Muslim revivalist movement. It is a new form of terrorism which is driven by a fanatical determination to inflict maximum civilian and economic damages. Although mainly targeting the West, the reckless operations of the GSJ have resulted in indiscriminate slaughter. The GSJ includes many terrorist groups from different countries forms a large global terrorist network. Through this network, the GSJ has successfully planned and launched many large-scale terrorist attacks across the world, including the 9/11 tragedy in 2001, the bombing in Bali in 2002, and the bombing in Morocco in 2003.

The data about the GSJ network were provided by the author of a recently published book, *Understanding the Terror Networks* (Sageman 2004). The author is a former Foreign Service officer who worked closely with Afghanistan's mujahedin from 1987 to 1989. The network was constructed based entirely on open-source information. In decreasing degrees of reliability, the information sources include transcripts of court proceedings involving GSJ terrorists and their organizations, reports of court proceedings, corroborated information from people with direct access to the information provided, uncorroborated statements from people with the access, and finally, statements from people who had heard the information second-hand (Sageman 2004). Information about all the nodes (terrorists) and links (relations) was scrutinized and carefully cross-validated.

The final dataset consists of the profile information of 366 GSJ terrorists which includes a set of sociological features (e.g., geographical origins, original socio-economic status, education, occupation, etc.) and individual psychological features (e.g., mental illness, personality, pathological narcissism, etc.) that could explain why these people became terrorists. More importantly, the data also captures all known relationships and interactions among these 366 GSJ terrorists. These relationships and interactions include personal relationships (e.g., acquaintance, friend, relative, and family member), religious relationships (following the same religious leader), operational interactions (participating in the same attacks), and other relationships. The dataset is presented in the form of a spreadsheet with each row containing the basic features of a certain GSJ member as well as all the other members that are related to this member through the various relationships or interactions mentioned above. Our network visualization provides an intuitive and clear view of the overall GSJ network (Fig. 1a).

However, as the author points out in the book, the data are subject to several limitations. First, the members included in the network may not be a representative sample of the Global Salafi Jihad as a whole. It is biased toward leaders and the members who have been captured or uncovered in executed attacks. Second, because most of the sources were based on retrospective accounts, the data may be subject to self-reported biases. Despite the limitations, the data have revealed stunning insights into the clandestine organizations of terrorists (Sageman 2004). More importantly, this dataset contains information about the time when each individual terrorist joined or left the network between 1989 and 2003, making it a good sample for studying the dynamic survival process of this terrorist organization.

To study the dynamics of the GSJ network during the 15-year period, we use both descriptive and simulation approaches. Like many descriptive studies on network dynamics (Barabási et al. 2002; Csányi and Szendroi 2004; Hajra and Sen 2005), we aim to capture and observe the changes in the network over time based on two topological statistics: average degree and degree distribution (Barabási et al. 2002). The degree of a node is the number of links it has. The degree distribution of a network, $P(k)$, is the probability that a node has exactly k links. The changes observed in the statistics are then plotted with respect to time in order to examine the dynamic patterns. In particular, the growth of a network can be described by its average degree. It is used to compare the growing speeds of links and nodes: if the average degree increases over time, the number of links grows faster than nodes, indicating accelerated growth (Albert and Barabási 2002).

In addition, we studied the robustness of the GSJ network by examining its structural changes under random and targeted attacks. Unlike most existing robustness studies (Albert et al. 2000; Cohen et al. 2000; Crucitti et al. 2003; Solé and Montoya 2001) which test network robustness based on a snapshot of the network assuming a single decaying mode, we examine the "dynamic robustness" of the network by allowing it to include new nodes when some nodes are removed. That is, the network can be in both growth and decay modes during its entire life span. Such a dynamic test is more realistic because the GSJ has never been in a single mode.

To examine the dynamic robustness of the network, we use the diameter l (Watts and Strogatz 1998) (Fig. 3b) to measure the interconnectedness of the network over time. The diameter of a network is defined as the average length of the shortest paths between any pair of nodes in the largest connected component of the network. In general, the shorter the diameter is, the more interconnected a network is. Removing a node usually will increase the diameter, since it may eliminate a link which is in the shortest path of another pair of nodes.

In our dynamic robustness test, we adopt three different node removal strategies: (a) random node removal (random errors) in which randomly selected nodes are removed; (b) preferential node removal (targeted attacks) in which the most connected nodes are removed; and (c) real node removal (authorities' counterattacks) in which nodes are removed in the same order as authorities arrested the terrorists in reality. The third removal strategy was possible because our dataset contains information about the exact time each terrorist died or was arrested.

Results and Discussion

The Growth Pattern

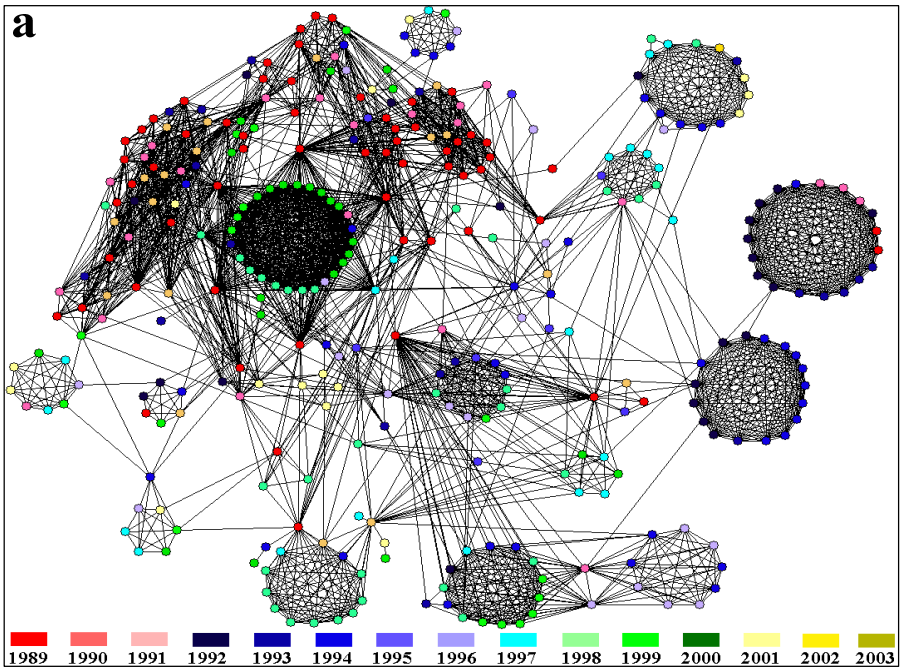
To study the growth patterns of the GSJ network, we measured the changes in the average degree from 1989 to 2003 (Table 1). We found that the GSJ network experienced three stages during its evolution: (I) the emerging stage from 1989 to 1991, during which the network was under accelerated growth in that the average degree drastically increased from 9.86 to 14.48; (II) the maturing stage from 1992 to 2000, during which the average degree first decreased a little to 13.86 and stayed relatively stable until 1997; it peaked at 14.54 in 2000; (III) the disintegrating stage from 2001 to 2003, during which the average degree dramatically decreased, indicating that the GSJ network started to fall apart as a large portion of nodes left the network. Figure 1 presents the visualizations of the network during the three stages.

During the emerging stage, three clusters emerged (Fig. 1b). The three clusters are defined mainly based on their geographical origins (Sageman 2004): the Central Staff cluster consisting of the leaders of Al Qaeda and the GSJ network including Bin Laden, the Southeast Asian cluster consisting of followers of Jemaah Islamiyan centered in Indonesia and Malaysia, and the Core Arabs cluster consisting of terrorists from Arab states (e.g., Saudi Arabia, Egypt, Yemen, and Kuwait). These three clusters are the backbone of the GSJ network.

To study the growth patterns in depth, we divided all the nodes into 12 yearly groups from 1989 to 2000, according to the year they joined the GSJ network (few nodes joined after 2000). We then measured the changes in the average degree of each yearly group from the year they joined the GSJ network to 2000 (Fig. 2). We found that the average degrees of the three groups that joined during the emerging stage (Fig. 2a) were generally larger than those of the groups that joined during the maturing stage (Fig. 2b). This is consistent with the original scale-free model in which older nodes have more advantage over younger nodes in acquiring links (Barabási and Albert 1999). This finding also shows that the

Stage	Year	No. of Nodes (n)	No. of Links (m)	Average Degree ($\frac{2m}{n}$)	R^2 of Regression Analysis on the Degree Distribution
I	1989	61	301	9.86	0.05
	1990	79	476	12.06	0.07
	1991	102	739	14.48	0.06
II	1992	124	859	13.86	0.17
	1993	142	1026	14.46	0.22
	1994	170	1163	13.68	0.21
	1995	166	1079	13	0.52
	1996	164	1040	12.68	0.48
	1997	183	1135	12.40	0.47
	1998	197	1240	12.58	0.63
	1999	194	1264	13.04	0.62
	2000	206	1498	14.54	0.48
III	2001	151	714	9.46	0.54
	2002	103	386	7.50	0.45
	2003	48	92	3.80	0.67

Table 1. The statistics describing the structural changes of the GSJ network from 1989 to 2003.



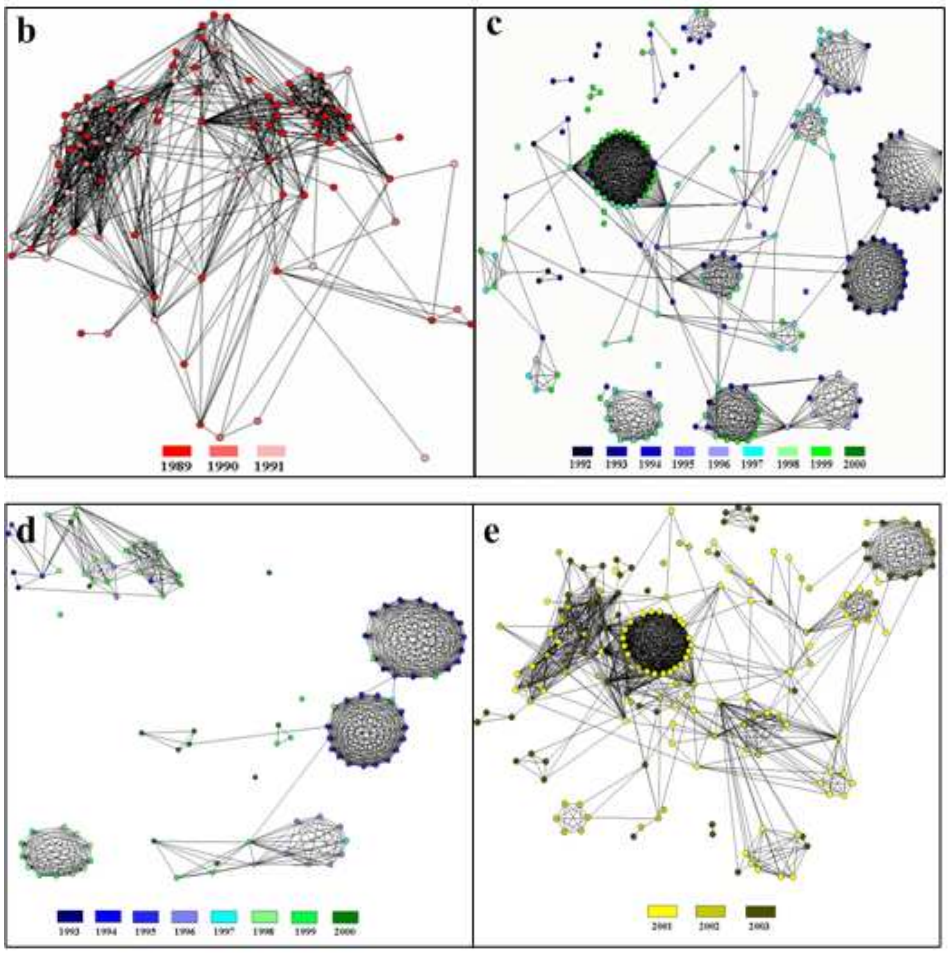
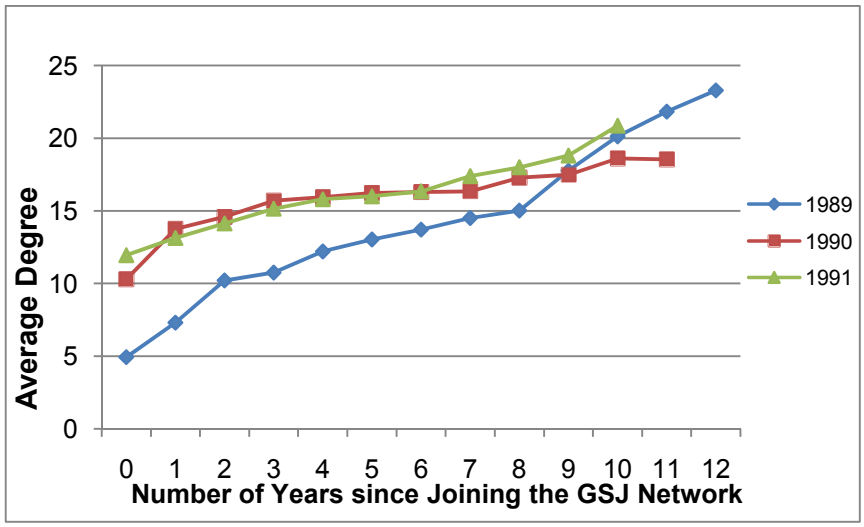


Fig.1. The dynamic view of the Global Salafi Jihad terrorist network. Nodes are color coded in terms of years. (a) The overall network with terrorists who joined the GSJ network from 1989 to 2003. (b) Terrorists who joined the network from 1989 to 1991. (c) Terrorists who joined the network from 1992 to 2000. (d) Terrorists who were arrested by authorities from 1993 to 2000. (e) Terrorists arrested from 2001 to 2003.

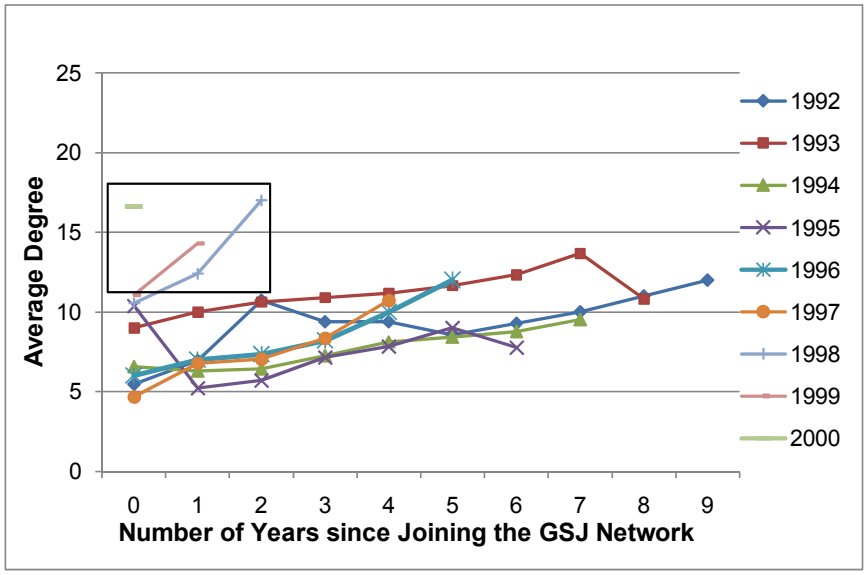
aging effect (Albert and Barabási 2002) which accounts for the situation where older nodes become less capable of acquiring new links due to age, did not compromise the effect of growth. Terrorists who joined the network early still establish relationships with new members and stay active in operations.

Interestingly, the average degrees of the three most recent groups that joined during the maturing stage increased much faster than the average degrees of other groups who joined earlier in this stage (Fig. 2b). This is mainly because the GSJ

network peaked in size around the end of the maturing stage (1998 - 2000). Hence those most recently joined nodes had more existing nodes available to connect to.



(a)



(b)

Fig.2. The changes in the average degrees of the 12 yearly groups (1989-2000) of terrorists from the year they joined the GSJ network to 2000. (a) The three yearly groups of terrorists who joined the GSJ network in 1989, 1990, and 1991, (b) The nine yearly groups who joined the GSJ network from 1992 to 2000.

We also found that the GSJ network presented scale-free features. We conducted regression analysis on the degree distribution of the GSJ network for each year and measured the goodness of fit (R^2) of the power-law distribution. The changes in R^2 (Table 1) for the regression analysis indicate that the GSJ network was rather random at the beginning and displayed more and more scale-free features over time.

The Evolution of the GSJ Network

We found that terrorists joined and left the GSJ network mainly on an operational base. An operation is a terrorist attack carried out by a group of terrorists, who are related to each other through operational links and formed an operational cluster. Examples of operations are the 9/11 attack in the U.S. and the Bali bombing in 2002. The maturing stage saw the network's most ambitious operations. During this stage, the network started recruiting new members and formed operational clusters to carry out terrorist attacks. In each year, most new members were involved in one or two terrorist attacks and most of these operational clusters were formed in one year or in two consecutive years. In addition, the node removal during this period followed a similar pattern. For example, 9 out of 13 members of the Aden (Yemen) terrorist attack in 1998 joined the GSJ network in the same year, and 12 of them were arrested immediately after the attack.

At the end of the maturing stage from 1998 to 2000, operations became more decentralized. According to Sageman (2004), field lieutenants and their local initiators, rather than the Central Staff took more responsibility for day-to-day operations during this period of time. Field lieutenants are important channels connecting operational clusters to the Central Staff. Most field lieutenants are highly connected hubs in the network. Moreover, the node removals (Fig. 1d) during this period became more severe: after a terrorist attack, most terrorist nodes in that operational cluster would be removed by authorities in a short time. Nevertheless, those field lieutenants usually tended to survive the first wave of counterattacks. This guaranteed the integrity of the main body of the GSJ network and diminished the effect of immediate counterattacks from authorities.

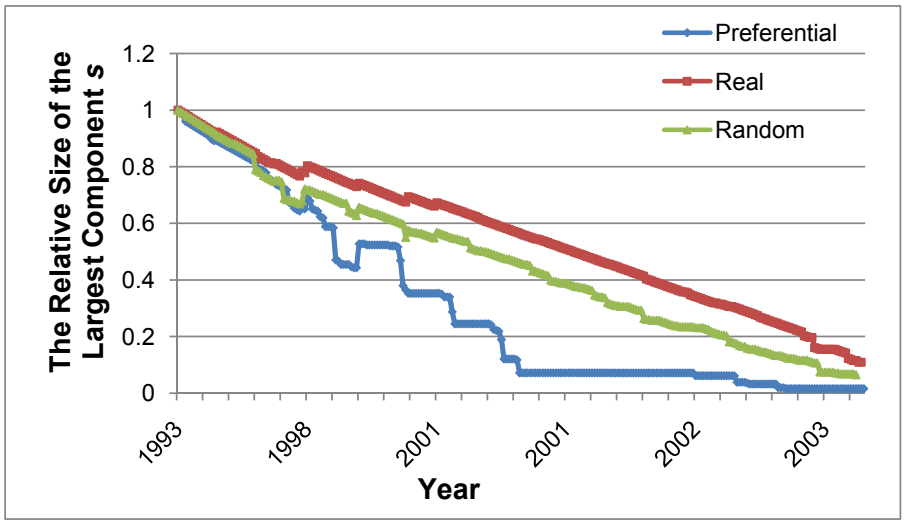
During the disintegrating stage (2001 to 2003) nearly 57% of the nodes in the GSJ network were removed. Unlike the maturing stage, the nodes removed in this stage included many highly connected hubs (Fig. 1e). The removal of these hubs caused the network to disintegrate into isolated cliques. This significantly weakened the network's communication ability and logistic support for large scale operations like the 9/11 attack (Sageman 2004).

Note that few nodes joined the network during the disintegrating stage. There are two possible reasons, namely, the elimination of the training camps in Afghanistan by U.S. forces and the lack of current information about the network.

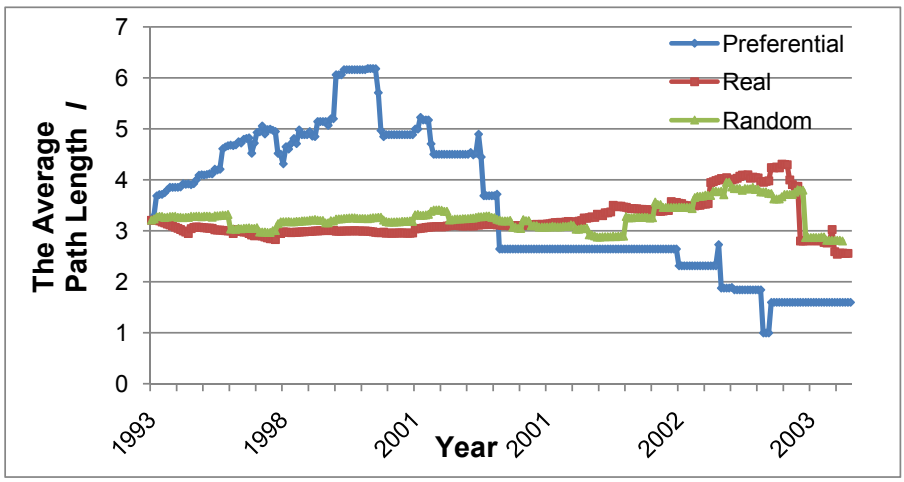
The first reason may significantly prevent the new recruitment of terrorists. The latter one could be a limitation of our dataset.

The Robustness

As mentioned above, we found that the GSJ network displayed more and more scale-free features over time. Thus we expected similar error tolerance and attack vulnerability (Albert et al. 2000) of scale-free networks in our dynamic robustness test.



(a)



(b)

Fig.3. The changes in (a) the relative size of the largest component *s*, and (b) the average path length *l* from 1993 to 2003.

We simulated the changes of the GSJ network from 1993 to 2003 with three different node removal strategies. For each year we used the three node removal strategies to remove the same number of nodes as were removed in reality. At the same time, we added nodes to the network based on the data. We did not analyze the robustness before 1993 because few nodes were removed from the network before then. We then measured the average path length l of the three simulated networks from 1993 to 2003 to study their robustness (Fig. 3b).

The responses of the GSJ network to these three different strategies were quite different. The network displays a strong robustness against random errors and real attacks from authorities during the maturing stage. The average path lengths (Fig. 3b) of both random node removal and real node removal generally remained unchanged during the maturing stage. As more than 50% of the nodes were removed, the diameters started to increase to their peaks (3.95 and 4.31 for the random and real removals, respectively). They then decreased, indicating the breakdown of the network.

The network was more vulnerable to targeted attacks than both random errors and real attacks. For the preferential node removal, l increased to a more prominent peak of 6.18 much faster than the other two strategies. This implies that the network efficiency is rapidly reduced by the loss of its key members because on average, each node needs to go through more intermediate nodes to interact with other nodes. The changes in the relative size (s) of the largest component of the network also confirm this finding (Fig. 3a): s decreased (the network fell apart) faster when using preferential node removal than using the random and real node removal. Moreover, we found that the real node removal was even less effective in disrupting the GSJ network than random node removal (Fig. 3a).

These distinct behaviors (error tolerance and attack vulnerability) of the GSJ network against different node removal strategies are rooted in the dynamical processes that occurred in the network. In each year the most newly joined nodes form one or two operational clusters, in which these nodes were fully interconnected with each other by operational relationships (links). A small number of these nodes had links to the nodes outside their operational clusters and became hubs in the network. The degrees of these hubs usually were much larger than that of other nodes in their operational clusters. As more and more new nodes entered in this way, nodes in the GSJ network became more and more heterogeneous in terms of degree over time. As a result, low degree nodes at the peripheral of operational clusters are far more abundant than highly connected hubs. Random node removal is more likely to destroy these peripheral nodes without affecting the main structure of the network (error tolerance). In contrast, preferential node removal of these hubs can drastically degrade the network by isolating operational clusters from the largest component (attack vulnerability).

The ineffectiveness of the real attacks, on the other hand, may be because highly connected hubs such as commanders and coordinators usually are more experienced and better protected than average terrorists, and thus are more difficult to apprehend. The probability of their being captured is lower than random chance. The possibility of their survival from authorities' counterattacks is much higher than the average.

Concluding Remarks

In this research we studied the evolution of the GSJ network to uncover the survival mechanisms of a terrorist organization. We found that three factors may have contributed to the survival of the network: growth, scale-free topology, and the ineffectiveness of the counterattack measures. The network experienced three distinct stages of growth from 1989 to 2003: emerging stage, maturing stage, and disintegrating stage. The network displayed different growth patterns in different stages. We found that the scale-free topology could partly account for the network's robustness, helping the network survive under constant counterattacks from authorities. The scale-free topology gradually emerged as new members joined in on an operational basis and the hubs acquired connections over time. On the other hand, the network could have remained active after numerous arrests of its members because the damages were localized within operations to a large extent. In addition, the leaders in the network are difficult to capture or remove and continue to function as hubs connecting members. Although numerous arrests and counterattacks have weakened the network, it still remains functional and has the potential to grow.

Note that findings in this study were obtained based only on the dataset about the Global Salafi Jihad and may not be generalized to other terrorist organizations. In addition, because of the possible data problems mentioned earlier, the results need further validation and verification. At this point we cannot draw definitive conclusions about the exact means by which terrorist organizations have survived over time. More reliable data and further research are needed to gain deeper insights into the underlying mechanisms for the survival of terrorist networks.

References

Albert, R. and Barabási, A.-L. (2002). "Statistical Mechanics of Complex Networks." *Reviews of Modern Physics* **74**(1): 47-97.

Albert, R., Jeong, H. and Barabasi, A.-L. (2000). "Error and attack tolerance of complex networks." *Nature* **406**(6794): 378-382.

Amaral, L. A. N., Scala, A., Barthelemy, M. and Stanley, H. E. (2000). "Classes of small-world networks." *Proceedings of the National Academy of Science of the United States of America* **97**: 11149-11152.

Barabási, A.-L. and Albert, A.-L. R. (1999). "Emergence of scaling in random networks." *Science* **286**(5439): 509-512.

Barabási, A.-L., Jeong, H., Zéda, Z., Ravasz, E., Schubert, A. and Vicsek, T. (2002). "Evolution of the social network of scientific collaborations." *Physica A* **311**: 590-614.

Broder, A., Kumar, R., Maghoul, F., Raghavan, P., Rajagopalan, S., State, R., Tomkins, A. and Wiener, J. (2000). "Graph structure in the web." *Computer Networks* **33**(1-6): 309-320.

Carley, K. M., Dombroski, M., Tsvetovat, M., Reminga, J. and Kamneva, N. (2003). *Destabilizing dynamic covert networks*. the 8th International Command and Control Research and Technology Symposium, Washington DC., VA.

Cohen, R., Erez, K., ben-Avraham, D. and Havlin, S. (2000). "Resilience of the internet to random breakdowns." *Physical Review Letters* **85**(21): 4626-4628.

Crucitti, P., Latora, V., Marchiori, M. and Rapisarda, A. (2003). "Efficiency of scale-free networks: Error and attack tolerance." *Physica A* **320**: 622-642.

Csányi, G. and Szendroi, B. (2004). "Structure of a large social network." *Physical Review E* **69**: 036131.

Dombroski, M. J. and Carley, K. M. (2002). "NETEST: Estimating a terrorist network's structure." *Computational & Mathematical Organization Theory* **8**: 235-241.

Faloutsos, M., Faloutsos, P. and Faloutsos, C. (1999). *On power-law relationships of the Internet topology*. Annual Conference of the Special Interest Group on Data Communication (SIGCOMM '99), Cambridge, MA.

Garlaschelli, D., Caldarelli, G. and Pietronero, L. (2003). "Universal scaling relations in food webs." *Nature* **423**(6936): 165-168.

Hajra, K. B. and Sen, P. (2005). "Aging in citation networks." *Physica A* **346**: 44-48.

Huberman, B. A. and Adamic, L. A. (1999). "Growth dynamics of the World-Wide Web." *Nature* **401**: 131.

Jeong, H., Tombor, B., Albert, R., Oltval, Z. N. and Barabási, A.-L. (2000). "The large-scale organization of metabolic networks." *Nature* **407**(6804): 651-654.

Klerks, P. (2001). "The network paradigm applied to criminal organizations: Theoretical nitpicking or a relevant doctrine for investigators? Recent developments in the Netherlands." *Connections* **24**(3): 53-65.

Krebs, V. E. (2001). "Mapping networks of terrorist cells." *Connections* **24**(3): 43-52.

Kumar, S. R., Raghavan, P., Rajagopalan, S. and Tomkins, A. (1999). "Trawling the web for emerging cyber-communities." *Computer Networks* **31**(11-16): 1481-1493.

Milward, H. B. and Raab, J. (2002). *Dark network: The structure, operation, and performance of international drug, terror, and arms trafficking networks*. International Conference on the Empirical Study of Covernance, Management, and Performance, Barcelona, Spain.

Newman, M. E. J. (2001). "The structure of scientific collaboration networks." *Proceedings of the National Academy of Science of the United States of America* **98**: 404-409.

Newman, M. E. J. (2004). "Coauthorship networks and patterns of scientific collaboration." *Proceedings of the National Academy of Science of the United States of America* **101**: 5200-5205.

Sageman, M. (2004). *Understanding Terror Networks*. Philadelphia, PA, University of Pennsylvania Press.

Solé, R. V. and Montoya, J. M. (2001). "Complexity and fragility in ecological networks." *Proceedings of the Royal Society B* **268**: 2039-2045.

Watts, D. J. and Strogatz, S. H. (1998). "Collective Dynamics of 'Small-World' Networks." *Nature* **393**: 440-442.